

# Transmitter Optimization in Slow Fading MISO Wiretap Channel

Sanjay Vishwakarma and A. Chockalingam

Email: sanvish1975@gmail.com, achockal@ece.iisc.ernet.in

Department of ECE, Indian Institute of Science, Bangalore 560012, India

**Abstract**—In this paper, we consider the transmitter optimization problem in slow fading multiple-input-single-output (MISO) wiretap channel. The source transmits a secret message intended for  $K$  users in the presence of  $J$  non-colluding eavesdroppers, and operates under a total power constraint. The channels between the source and all users and eavesdroppers are assumed to be slow fading, and only statistical channel state information (CSI) is known at the source. For a given code rate and secrecy rate pair of the wiretap code, denoted by  $(R_D, R_s)$ , we define the non-outage event as the joint event of the link information rates to  $K$  users be greater than or equal to  $R_D$  and the link information rates to  $J$  eavesdroppers be less than or equal to  $(R_D - R_s)$ . We minimize the transmit power subject to the total power constraint and satisfying the probability of the non-outage event to be greater than or equal to a desired threshold  $(1 - \epsilon)$ .

**keywords:** Physical layer security, MISO wiretap channel, secrecy rate, multiple eavesdroppers, slow fading.

## I. INTRODUCTION

With growing applications on wireless networks, there is a need to provide security, along with reliability, from being eavesdropped, which can easily happen due to the broadcast nature of the wireless transmission. Wyner, in his work in [1], showed that a message could be transmitted at a rate called secrecy rate, at which the legitimate user could decode the message reliably whereas the eavesdropper could be kept entirely ignorant. The wiretap channel model in [1] was physically degraded and discrete memoryless. Later, the work in [1] was extended to more general broadcast channel and Gaussian channel in [2] and [3], respectively. Subsequent extension to various multi-antenna wireless wiretap channels and the corresponding achievable secrecy rates and secrecy capacities have been reported by many authors, e.g., [4]–[11].

In [12], secrecy capacity of a quasi-static single-antenna Rayleigh fading channel in terms of outage probability has been characterized. Outage probability characterization of the secrecy rate of multiple-input-single-output (MISO) wiretap channel with artificial noise has been reported in [13]–[15], and that of amplify-and-forward relay channel has been reported in [16]. Motivated by the need for outage probability characterization of secrecy rate in MISO wiretap channel, in this paper, we consider the transmitter optimization problem in slow fading MISO wiretap channel. The source transmits a secret message intended for  $K$  users in the presence of  $J$  non-colluding eavesdroppers, and operates under a total power constraint. The channels between the source and all users and eavesdroppers are assumed to be slow fading. Only statistical channel state information (CSI) is assumed to be known at the source. For a given code rate and secrecy rate pair of the

wiretap code, denoted by  $(R_D, R_s)$ , we define the non-outage event as the joint event of the link information rates to  $K$  users be greater than or equal to  $R_D$  and the link information rates to  $J$  eavesdroppers be less than or equal to  $(R_D - R_s)$ . We minimize the transmit power subject to the total power constraint and satisfying the probability of the non-outage event to be greater than or equal to a desired threshold  $(1 - \epsilon)$ . We obtain the achievable  $(R_D, R_s)$  region and the transmit beamforming vector. We note that we differ from the reported works in [13,14], which also consider multiple eavesdroppers scenario, in following aspects: *i*) number of users  $K$  can be more than one, *ii*) only statistical CSI of the users channels are known, and *iii*) channel covariance matrices of all users and eavesdroppers can be arbitrary positive semidefinite matrices.

**Notations :**  $\mathbf{A} \in \mathbb{C}^{N_1 \times N_2}$  implies that  $\mathbf{A}$  is a complex matrix of dimension  $N_1 \times N_2$ .  $\mathbf{A} \succeq \mathbf{0}$  and  $\mathbf{A} \succ \mathbf{0}$  imply that  $\mathbf{A}$  is a positive semidefinite matrix and positive definite matrix, respectively. Identity matrix is denoted by  $\mathbf{I}$ . Transpose and complex conjugate transpose operations are denoted by  $[\cdot]^T$  and  $[\cdot]^*$ , respectively.  $\mathbb{E}[\cdot]$  denotes the expectation operator, and  $\|\cdot\|$  denotes the 2-norm operator.  $\text{diag}(\mathbf{a})$  denotes a diagonal matrix with elements of the vector  $\mathbf{a} \in \mathbb{C}^{N \times 1}$  on its diagonal. Trace of matrix  $\mathbf{A} \in \mathbb{C}^{N \times N}$  is denoted by  $\text{Tr}(\mathbf{A})$ .  $\mathbf{h} \in \mathbb{C}^{N \times 1} \sim \mathcal{CN}(\mathbf{0}, \mathbf{H})$  implies that  $\mathbf{h}$  is a circularly symmetric complex Gaussian random vector with mean vector  $\mathbf{0}$  and covariance matrix  $\mathbf{H}$ .

## II. SYSTEM MODEL

Consider a MISO wiretap channel as shown in Fig. 1, which consists of a source  $S$  having  $N$  transmit antennas,  $K$  users  $\{D_1, D_2, \dots, D_K\}$  each having single antenna, and  $J$  non-colluding eavesdroppers  $\{E_1, E_2, \dots, E_J\}$  each having single antenna. The complex channel gain vector from  $S$  to  $D_k$  is denoted by  $\mathbf{h}_k \in \mathbb{C}^{1 \times N}$ ,  $1 \leq k \leq K$ . Likewise, the complex channel gain vector from  $S$  to  $E_j$  is denoted by  $\mathbf{z}_j \in \mathbb{C}^{1 \times N}$ ,  $1 \leq j \leq J$ . We assume that the channels between  $S$  to  $D_k$ s and those between  $S$  to  $E_j$ s fade slowly and independently with  $\mathbf{h}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{H}_k)$ , and  $\mathbf{z}_j \sim \mathcal{CN}(\mathbf{0}, \mathbf{Z}_j)$ . These channel gains are assumed to be unknown at  $S$ . We assume that the source  $S$  operates under total power constraint  $P_T$ . The communication between  $S$  and  $D_k$ s happens in  $n$  channel uses. The source  $S$  transmits secret message  $W$  which is equiprobable over  $\{1, 2, \dots, 2^{nR_s}\}$ . For each  $W$  drawn equiprobably from the set  $\{1, 2, \dots, 2^{nR_s}\}$ , the source, using a stochastic encoder, maps  $W$  to a codeword  $\{x_i\}_{i=1}^n$  of length  $n$ , where each  $x_i \in \mathbb{C}$ , i.i.d.  $\sim \mathcal{CN}(0, 1)$ , and  $\mathbb{E}[|x_i|^2] = 1$ . Each codeword  $\{x_i\}_{i=1}^n$  belongs to a collection of  $2^{nR_D}$

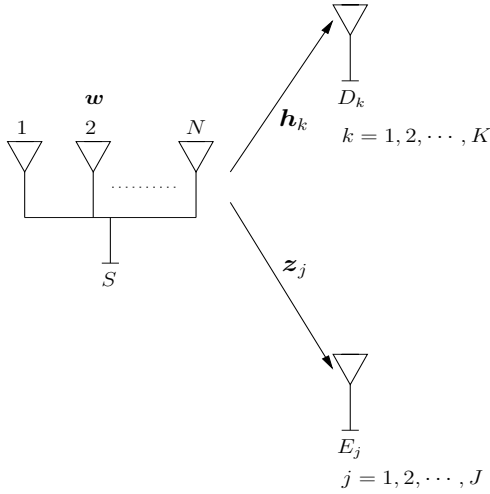


Fig. 1. System model for MISO wiretap channel with  $K$  users and  $J$  eavesdroppers.

codewords (i.e., wiretap code) where  $R_D \geq R_s$ . The source applies the complex weight  $\mathbf{w} = [w_1, w_2, \dots, w_N]^T \in \mathbb{C}^{N \times 1}$  and transmits the weighted symbol which is  $\mathbf{w}x_i$  in the  $i$ th channel use,  $1 \leq i \leq n$ . Since the source is power constrained, this implies that

$$\|\mathbf{w}\|^2 \leq P_T. \quad (1)$$

In the following, we will use  $x$  to denote the symbols in the codeword  $\{x_i\}_{i=1}^n$ . Since the channel is slow fading and the CSI is unknown at the source  $S$ , we define the non-outage event for a given  $(R_D, R_s)$  pair of the wiretap code, denoted by  $\mathcal{E}$ , and impose the probability constraint on  $\mathcal{E}$  as follows:

$$\mathcal{E} = \left\{ R_{D_k} \geq R_D, \quad \forall k = 1, 2, \dots, K, \quad \text{and} \right. \\ \left. R_D - R_s \geq R_{E_j}, \quad \forall j = 1, 2, \dots, J \right\}, \quad (2)$$

$$\Pr(\mathcal{E}) \geq (1 - \epsilon), \quad (3)$$

where  $(1 - \epsilon)$  is the non-outage probability threshold, and  $R_{D_k}$  and  $R_{E_j}$  are the link information rates between  $S$  to  $D_k$  and  $S$  to  $E_j$ , respectively. In other words, when the source selects the target code rate and target secrecy rate pair of the wiretap code as  $(R_D, R_s)$ , the above constraint implies that, with probability greater than or equal to  $(1 - \epsilon)$ , all  $D_k$ s will be able to successfully decode the transmitted message while all  $E_j$ s will be ignorant about the transmitted message. We also note that when the CSI on all the links are known at  $S$ , the achievability of the secrecy rate  $R_s$  is shown in [11]. Let  $y_{D_k}$  and  $y_{E_j}$  denote the received signals at  $D_k$  and  $E_j$ , respectively. We have

$$y_{D_k} = \mathbf{h}_k \mathbf{w} x + \eta_{D_k}, \quad \forall k = 1, 2, \dots, K, \quad (4)$$

$$y_{E_j} = \mathbf{z}_j \mathbf{w} x + \eta_{E_j}, \quad \forall j = 1, 2, \dots, J, \quad (5)$$

where  $\eta$ s are noise components, assumed to be i.i.d.  $\sim \mathcal{CN}(0, N_0)$ .

### III. TRANSMITTER OPTIMIZATION UNDER SECRECY CONSTRAINT

Using (4) and (5), and for a given  $\mathbf{h}_k$  and  $\mathbf{z}_j$ , the information rates at  $D_k$  and  $E_j$  are obtained, respectively, as follows:

$$R_{D_k} = I(x; y_{D_k}) = \log_2 \left( 1 + \frac{|\mathbf{h}_k \mathbf{w}|^2}{N_0} \right), \quad (6)$$

$$R_{E_j} = I(x; y_{E_j}) = \log_2 \left( 1 + \frac{|\mathbf{z}_j \mathbf{w}|^2}{N_0} \right). \quad (7)$$

Further, subject to the constraints in (1) and (3) and using (6) and (7), the optimization problem to minimize the transmit power is as follows:

$$\min_{\mathbf{w}} \|\mathbf{w}\|^2 \quad (8)$$

$$\text{s.t.} \quad \|\mathbf{w}\|^2 \leq P_T, \quad (9)$$

$$\Pr \left\{ \log_2 \left( 1 + \frac{|\mathbf{h}_k \mathbf{w}|^2}{N_0} \right) \geq R_D, \quad \forall k = 1, 2, \dots, K, \right. \\ \left. R_D - R_s \geq \log_2 \left( 1 + \frac{|\mathbf{z}_j \mathbf{w}|^2}{N_0} \right), \quad \forall j = 1, 2, \dots, J \right\} \\ \geq (1 - \epsilon). \quad (10)$$

Since  $\mathbf{h}_k$ s and  $\mathbf{z}_j$ s are independent, we rewrite the constraint (10) in the following equivalent product form:

$$\prod_{k=1}^K \Pr \left\{ |\mathbf{h}_k \mathbf{w}|^2 \geq (2^{R_D} - 1)N_0 \right\} \\ \prod_{j=1}^J \Pr \left\{ |\mathbf{z}_j \mathbf{w}|^2 \leq (2^{(R_D - R_s)} - 1)N_0 \right\} \geq (1 - \epsilon). \quad (11)$$

We note that solving the optimization problem (8) in its original form is hard. So, in order to simplify the analysis, we replace the product probability constraint in (11) with the following  $K + J$  individual probability constraints:

$$\forall k = 1, 2, \dots, K, \quad \text{and} \quad \forall j = 1, 2, \dots, J,$$

$$\Pr \left\{ |\mathbf{h}_k \mathbf{w}|^2 \geq (2^{R_D} - 1)N_0 \right\} \geq (1 - \epsilon)^{\frac{1}{K+J}}, \quad (12)$$

$$\Pr \left\{ |\mathbf{z}_j \mathbf{w}|^2 \leq (2^{(R_D - R_s)} - 1)N_0 \right\} \geq (1 - \epsilon)^{\frac{1}{K+J}}. \quad (13)$$

We also note that any  $\mathbf{w}$  which satisfies all  $K + J$  constraints in (12) and (13) will also satisfy the product probability constraint in (11). However, the converse may not always be true. Further, since  $\mathbf{h}_k \mathbf{w}$  in (12) and  $\mathbf{z}_j \mathbf{w}$  in (13) are linear transformations of circularly symmetric complex Gaussian random vectors,  $\mathbf{h}_k \mathbf{w}$  and  $\mathbf{z}_j \mathbf{w}$  are also circularly symmetric complex Gaussian random variables, i.e.,  $\mathbf{h}_k \mathbf{w} \sim \mathcal{CN}(0, \mathbf{w}^* \mathbf{H}_k \mathbf{w})$ , and  $\mathbf{z}_j \mathbf{w} \sim \mathcal{CN}(0, \mathbf{w}^* \mathbf{Z}_j \mathbf{w})$ . This further implies that  $|\mathbf{h}_k \mathbf{w}|^2$  and  $|\mathbf{z}_j \mathbf{w}|^2$  are exponential random variables, i.e.,

$$|\mathbf{h}_k \mathbf{w}|^2 \sim \frac{1}{\mathbf{w}^* \mathbf{H}_k \mathbf{w}} \exp^{-\frac{\lambda}{\mathbf{w}^* \mathbf{H}_k \mathbf{w}}}, \quad \lambda \geq 0, \quad (14)$$

$$|\mathbf{z}_j \mathbf{w}|^2 \sim \frac{1}{\mathbf{w}^* \mathbf{Z}_j \mathbf{w}} \exp^{-\frac{\lambda}{\mathbf{w}^* \mathbf{Z}_j \mathbf{w}}}, \quad \lambda \geq 0. \quad (15)$$

Using (14) and (15), and by following standard integration steps, we get the following equivalent simplified inequalities for the probability constraints in (12) and (13):

$$\forall k = 1, 2, \dots, K, \quad \mathbf{w}^* \mathbf{H}_k \mathbf{w} \geq a, \quad (16)$$

$$\forall j = 1, 2, \dots, J, \quad \mathbf{w}^* \mathbf{Z}_j \mathbf{w} \leq b, \quad (17)$$

where  $a = \frac{(2^{R_D}-1)N_0}{-\ln(1-\epsilon)^{\frac{1}{K+J}}}$  and  $b = \frac{(2^{(R_D-R_s)}-1)N_0}{-\ln(1-(1-\epsilon)^{\frac{1}{K+J}})}$ . Replacing the constraint in (11) with (16) and (17), we get the following upper bound for the optimization problem (8):

$$\min_{\mathbf{w}} \|\mathbf{w}\|^2 \quad (18)$$

$$\text{s.t.} \quad \|\mathbf{w}\|^2 \leq P_T, \quad (19)$$

$$\forall k = 1, 2, \dots, K, \quad \mathbf{w}^* \mathbf{H}_k \mathbf{w} \geq a, \quad (20)$$

$$\forall j = 1, 2, \dots, J, \quad \mathbf{w}^* \mathbf{Z}_j \mathbf{w} \leq b, \quad (21)$$

We solve the above problem for the following two cases.

#### A. All $\mathbf{H}_k$ s and $\mathbf{Z}_j$ s are diagonal matrices

When all  $\mathbf{H}_k$ s and  $\mathbf{Z}_j$ s are diagonal positive semidefinite matrices, the optimization problem (18) can be written as the following equivalent linear optimization problem:

$$\min_{P_1, P_2, \dots, P_N} \sum_{m=1}^N P_m \quad (22)$$

$$\text{s.t.} \quad \forall m = 1, 2, \dots, N, \quad P_m \geq 0, \quad \sum_{m=1}^N P_m \leq P_T, \quad (23)$$

$$\forall k = 1, 2, \dots, K, \quad \sum_{m=1}^N P_m H_k^{mm} \geq a, \quad (24)$$

$$\forall j = 1, 2, \dots, J, \quad \sum_{m=1}^N P_m Z_j^{mm} \leq b, \quad (25)$$

where  $P_m = |w_m|^2$ ,  $\mathbf{H}_k = \text{diag}([H_k^{11}, H_k^{22}, \dots, H_k^{NN}]^T) \succeq \mathbf{0}$ , and  $\mathbf{Z}_j = \text{diag}([Z_j^{11}, Z_j^{22}, \dots, Z_j^{NN}]^T) \succeq \mathbf{0}$ . The above problem can be easily solved using linear optimization techniques. Having obtained  $P_1, P_2, \dots, P_N$ , the beamforming vector  $\mathbf{w}$  is  $[\sqrt{P_1}, \sqrt{P_2}, \dots, \sqrt{P_N}]^T$ .

#### B. Some of $\mathbf{H}_k$ s or $\mathbf{Z}_j$ s are not diagonal matrices

Here, we consider the general case when  $\mathbf{H}_k$ s and  $\mathbf{Z}_j$ s are Hermitian positive semidefinite matrices and some of  $\mathbf{H}_k$ s or  $\mathbf{Z}_j$ s are not diagonal. Define  $\mathbf{W} \triangleq \mathbf{w}\mathbf{w}^*$ . We rewrite the optimization problem (18) into the following equivalent form:

$$\min_{\mathbf{W}} \text{Tr}(\mathbf{W}) \quad (26)$$

$$\text{s.t.} \quad \mathbf{W} \succeq \mathbf{0}, \quad \text{rank}(\mathbf{W}) = 1, \quad \text{Tr}(\mathbf{W}) \leq P_T, \quad (27)$$

$$\forall k = 1, 2, \dots, K, \quad \text{Tr}(\mathbf{W}\mathbf{H}_k) \geq a, \quad (28)$$

$$\forall j = 1, 2, \dots, J, \quad \text{Tr}(\mathbf{W}\mathbf{Z}_j) \leq b. \quad (29)$$

The above optimization problem is a non-convex optimization problem. However, by relaxing the  $\text{rank}(\mathbf{W}) = 1$  constraint,

the above problem can be solved using semidefinite programming techniques [17]. But the solution  $\mathbf{W}$  of the above rank relaxed optimization problem may not have rank 1. This can be easily seen from the KKT conditions of the rank relaxed optimization problem which we discuss in the Appendix. We now take the rank-1 approximation as follows. Let  $\mathbf{w}_0$  be the unit-norm eigen direction corresponding to the largest eigen value of  $\mathbf{W}$ . We substitute  $\mathbf{W} = P\mathbf{w}_0\mathbf{w}_0^*$  in the above rank relaxed optimization problem and solve the resulting linear optimization problem for unknown  $P$ , i.e.,

$$\min_P P \quad (30)$$

$$\text{s.t.} \quad 0 \leq P \leq P_T, \quad (31)$$

$$\forall k = 1, 2, \dots, K, \quad P\mathbf{w}_0^* \mathbf{H}_k \mathbf{w}_0 \geq a, \quad (32)$$

$$\forall j = 1, 2, \dots, J, \quad P\mathbf{w}_0^* \mathbf{Z}_j \mathbf{w}_0 \leq b. \quad (33)$$

Having obtained the transmit power  $P$  from (30), the beamforming vector is  $\sqrt{P}\mathbf{w}_0$ .

*Remark 1:* We note that when the channel CSI  $\mathbf{h}_k$  on all  $D_k$ s are perfectly known at the source  $S$ , the constraints (28) and (29) in the optimization problem (26) should be replaced with the following constraints, respectively:

$$\text{Tr}(\mathbf{W}\mathbf{h}_k^* \mathbf{h}_k) \geq (2^{R_D} - 1)N_0, \quad (34)$$

$$\text{Tr}(\mathbf{W}\mathbf{Z}_j) \leq \frac{(2^{(R_D-R_s)} - 1)N_0}{-\ln(1 - (1-\epsilon)^{\frac{1}{J}})}. \quad (35)$$

*Remark 2:* When the source transmits the symbol  $x$  from an equiprobable complex finite alphabet set  $\mathbb{A} = \{a_1, a_2, \dots, a_M\}$  of size  $M$  (e.g.,  $M$ -ary) with  $\mathbb{E}[x] = 0$  and  $\mathbb{E}[|x|^2] = 1$ , the information rates in (6) and (7) can be written in the following forms, respectively:

$$R_{D_k} = I(x; y_{D_k}) = I\left(\frac{|\mathbf{h}_k \mathbf{w}|^2}{N_0}\right), \quad (36)$$

$$R_{E_j} = I(x; y_{E_j}) = I\left(\frac{|\mathbf{z}_j \mathbf{w}|^2}{N_0}\right), \quad (37)$$

where

$$I(\rho) \triangleq \frac{1}{M} \sum_{l=1}^M \int p_n(y - \sqrt{\rho} a_l) \log_2 \frac{p_n(y - \sqrt{\rho} a_l)}{\frac{1}{M} \sum_{m=1}^M p_n(y - \sqrt{\rho} a_m)} dy, \quad (38)$$

and  $p_n(\theta) = \frac{1}{\pi} e^{-|\theta|^2}$ . Using the fact that the mutual information function,  $I(\rho)$ , is a strictly-increasing concave function in  $\rho$  [18,19],  $K + J$  constraints in (20) and (21) can be written in the following forms, respectively:

$$\forall k = 1, 2, \dots, K, \quad \mathbf{w}^* \mathbf{H}_k \mathbf{w} \geq a, \quad (39)$$

$$\forall j = 1, 2, \dots, J, \quad \mathbf{w}^* \mathbf{Z}_j \mathbf{w} \leq b, \quad (40)$$

where  $a = \frac{I^{-1}(R_D)N_0}{-\ln(1-\epsilon)^{\frac{1}{K+J}}}$  and  $b = \frac{I^{-1}(R_D-R_s)N_0}{-\ln(1-(1-\epsilon)^{\frac{1}{K+J}})}$ . With finite alphabet input, the optimization problem (18) should be solved subject to the constraints in (39) and (40).

#### IV. RESULTS AND DISCUSSIONS

We have evaluated the secrecy rate through simulation with the following system parameters:  $N = 3$ ,  $K = 2$ ,  $J = 1, 2, 3$ ,  $N_0 = 1$ ,  $\epsilon = 0.1$ , and  $P_T = 12$  dB. We consider the scenarios discussed in Section III-A and Section III-B.

*Scenario of Section III-B:* We have used the following positive definite channel covariance matrices in the simulations:

$$\mathbf{H}_1 = \begin{bmatrix} 2.1670, & 0.1806 + 0.0183i, & -0.1453 - 0.3101i \\ 0.1806 - 0.0183i, & 1.9165, & 0.0696 + 0.3374i \\ -0.1453 + 0.3101i, & 0.0696 - 0.3374i, & 1.4180 \end{bmatrix} \succ \mathbf{0} \quad (41)$$

$$\mathbf{H}_2 = \begin{bmatrix} 1.9834, & -0.2001 + 0.0250i, & 0.0470 - 0.3424i \\ -0.2001 - 0.0250i, & 1.3867, & 0.0149 - 0.2083i \\ 0.0470 + 0.3424i, & 0.0149 + 0.2083i, & 1.4323 \end{bmatrix} \succ \mathbf{0} \quad (42)$$

$$\mathbf{Z}_1 = \begin{bmatrix} 0.0043, & 0.0010 - 0.0003i, & 0.0013 + 0.0009i \\ 0.0010 + 0.0003i, & 0.0074, & -0.0011 - 0.0029i \\ 0.0013 - 0.0009i, & -0.0011 + 0.0029i, & 0.0079 \end{bmatrix} \succ \mathbf{0} \quad (43)$$

$$\mathbf{Z}_2 = \begin{bmatrix} 0.0069, & 0.0004 - 0.0029i, & -0.0014 + 0.0014i \\ 0.0004 + 0.0029i, & 0.0070, & -0.0019 - 0.0002i \\ -0.0014 - 0.0014i, & -0.0019 + 0.0002i, & 0.0086 \end{bmatrix} \succ \mathbf{0} \quad (44)$$

$$\mathbf{Z}_3 = \begin{bmatrix} 0.0090, & -0.0026 + 0.0006i, & 0.0011 - 0.0009i \\ -0.0026 - 0.0006i, & 0.0064, & -0.0013 + 0.0018i \\ 0.0011 + 0.0009i, & -0.0013 - 0.0018i, & 0.0054 \end{bmatrix} \succ \mathbf{0} \quad (45)$$

For a given  $(R_D, R_s)$  pair, we solve the semidefinite rank relaxed optimization problem (26) using the tools in [20,21]. We numerically observe that, for any feasible  $(R_D, R_s)$  pair, the solution  $\mathbf{W}$  of the rank relaxed optimization problem (26) has rank 1. This implies that for such channel realizations, rank-1 approximation is not needed. In Fig 2(a), we plot

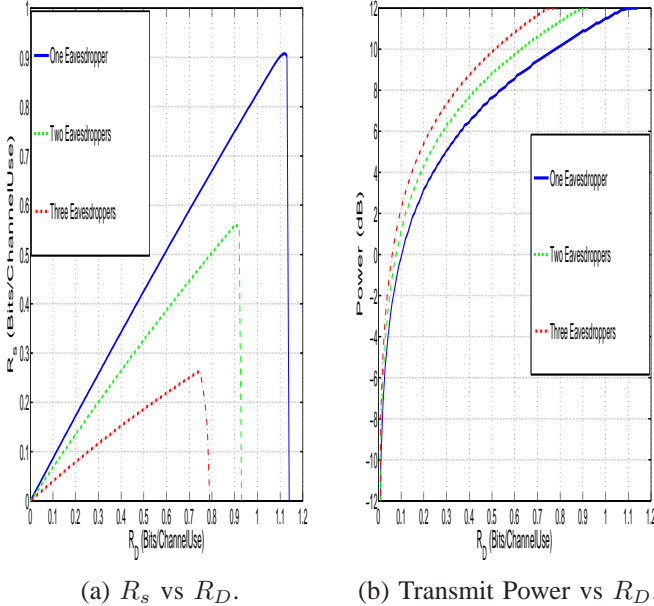


Fig. 2.  $R_s$  vs  $R_D$  and Transmit Power vs  $R_D$  in MISO wiretap channel with  $N = 3$ ,  $K = 2$ ,  $J = 1, 2, 3$ ,  $N_0 = 1$ ,  $\epsilon = 0.1$  and  $P_T = 12$  dB, and non-diagonal covariance matrices.

the maximum achievable  $R_s$  vs  $R_D$ . In Fig 2(b), we plot the corresponding minimum transmit power vs  $R_D$ . We

observe that the maximum achievable secrecy rate  $R_s$  and the corresponding minimum transmit power increases with increase in  $R_D$ . The secrecy rate drops to zero when the entire available power,  $P_T = 12$  dB, is used.

*Scenario of Section III-A:* Here, we take  $\mathbf{H}_1$ ,  $\mathbf{H}_2$ ,  $\mathbf{Z}_1$ ,  $\mathbf{Z}_2$ , and  $\mathbf{Z}_3$  as the diagonal approximation of covariance matrices in (41), (42), (43), (44), and (45), respectively. We solve the linear optimization problem (22) using the tools in [20,21], and we plot the maximum achievable  $R_s$  vs  $R_D$  and the corresponding minimum transmit power vs  $R_D$  in Fig 3(a) and Fig 3(b), respectively. As in Fig 2(a) and Fig 2(b), we

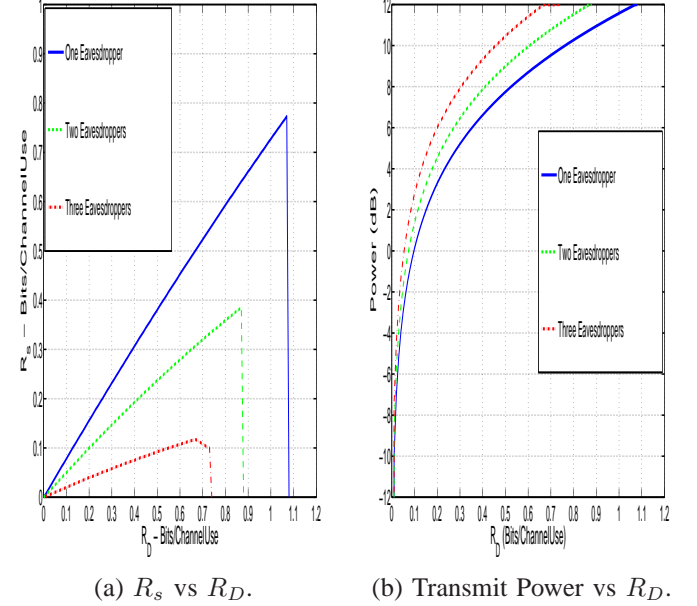


Fig. 3.  $R_s$  vs  $R_D$  and Transmit Power vs  $R_D$  in MISO wiretap channel with  $N = 3$ ,  $K = 2$ ,  $J = 1, 2, 3$ ,  $N_0 = 1$ ,  $\epsilon = 0.1$  and  $P_T = 12$  dB, and diagonal covariance matrices.

observe that the maximum achievable secrecy rate  $R_s$  and the corresponding minimum transmit power increases with increase in  $R_D$ . The secrecy rate drops to zero when the entire available power,  $P_T = 12$  dB, is used.

#### V. CONCLUSIONS

We considered the transmitter optimization problem in slow fading MISO wiretap channel. Secret message transmitted by the source was intended for  $K$  users in the presence of  $J$  eavesdroppers. For a given code rate and secrecy rate pair of the wiretap code, denoted by  $(R_D, R_s)$ , we defined the non-outage event and minimized the transmit power subject to the total power constraint and satisfying the probability of the non-outage event to be greater than a desired threshold  $(1 - \epsilon)$ . We obtained the achievable  $(R_D, R_s)$  region and the transmit beamforming vector.

#### APPENDIX

In this appendix, we analyze the rank of the optimal solution  $\mathbf{W}$  of the rank relaxed optimization problem (26). We take the



Lagrangian [17] of the rank relaxed optimization problem (26) as follows:

$$\begin{aligned} \ell(\mathbf{W}, \mathbf{\Lambda}, \lambda, \mu_k, \nu_j) = & \text{Tr}(\mathbf{W}) - \text{Tr}(\mathbf{\Lambda W}) \\ & + \lambda(\text{Tr}(\mathbf{W}) - P_T) + \sum_{k=1}^K \mu_k(a - \text{Tr}(\mathbf{W H}_k)) \\ & + \sum_{j=1}^J \nu_j(\text{Tr}(\mathbf{W Z}_j) - b), \quad (46) \end{aligned}$$

where  $\mathbf{\Lambda} \succeq \mathbf{0}$ ,  $\lambda \geq 0$ ,  $\mu_k \geq 0$ , and  $\nu_j \geq 0$  are Lagrangian multipliers. The KKT conditions are as follows:

- K1. All the constraints in (27), (28), and (29) excluding the constraint  $\text{rank}(\mathbf{W}) = 1$ ,
- K2.  $\text{Tr}(\mathbf{\Lambda W}) = 0$ . Since  $\mathbf{\Lambda} \succeq \mathbf{0}$  and  $\mathbf{W} \succeq \mathbf{0}$ , this implies that  $\mathbf{\Lambda W} = \mathbf{0}$ ,
- K3.  $\lambda(\text{Tr}(\mathbf{W}) - P_T) = 0$ ,
- K4.  $\forall k = 1, 2, \dots, K, \quad \mu_k(a - \text{Tr}(\mathbf{W H}_k)) = 0$ ,
- K5.  $\forall j = 1, 2, \dots, J, \quad \nu_j(\text{Tr}(\mathbf{W Z}_j) - b) = 0$ ,
- K6.  $\frac{\partial \ell}{\partial \mathbf{W}} = \mathbf{0}$  implies that  $\mathbf{\Lambda} = (1 + \lambda)\mathbf{I} - \sum_{k=1}^K \mu_k \mathbf{H}_k + \sum_{j=1}^J \nu_j \mathbf{Z}_j \succeq \mathbf{0}$ ,

The KKT conditions (K2), (K6), (K4), and (K5) imply that  $(1 + \lambda)\text{Tr}(\mathbf{W}) - \sum_{k=1}^K \mu_k a + \sum_{j=1}^J \nu_j b = 0$ . For  $\mathbf{W} \neq \mathbf{0}$ , this further implies that not all  $\mu_k$ s can be zero simultaneously. With this, we rewrite (K6) in the following form:

$$\mathbf{\Lambda} + \sum_{k=1}^K \mu_k \mathbf{H}_k = (1 + \lambda)\mathbf{I} + \sum_{j=1}^J \nu_j \mathbf{Z}_j \succ \mathbf{0}. \quad (47)$$

The above equation implies that  $\text{rank}(\mathbf{\Lambda} + \sum_{k=1}^K \mu_k \mathbf{H}_k) = N$ . This further implies that  $\text{rank}(\mathbf{\Lambda}) \geq N - \text{rank}(\sum_{k=1}^K \mu_k \mathbf{H}_k)$ . (K2) implies that  $\text{rank}(\mathbf{W}) \leq \text{rank}(\sum_{k=1}^K \mu_k \mathbf{H}_k)$  (assuming  $\mathbf{W} \neq \mathbf{0}$ ). This means that the rank of  $\mathbf{W}$  may not be one.

For the special case when  $K = 1$  and  $\mathbf{H}_1$  is a rank one positive semidefinite matrix, (47) implies that  $\text{rank}(\mathbf{\Lambda}) \geq N - 1$ . Assuming  $\mathbf{W} \neq \mathbf{0}$ , (K2) further implies that  $\text{rank}(\mathbf{\Lambda}) = N - 1$ , and  $\text{rank}(\mathbf{W}) = 1$ .

## REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.
- [2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 339-348, May 1978.
- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 451-456, Jul. 1978.
- [4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, NOW Publishers, vol. 5, no. 4-5, 2009.
- [5] Z. Li, R. Yates, and W. Trappe, "Secure communication with a fading eavesdropper channel," *Proc. IEEE ISIT'2007*, Jun. 2007.
- [6] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraint," *Proc. IEEE ISIT'2007*, Jun. 2007.
- [7] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.
- [8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Proc. IEEE ISIT'2008*, Jul. 2008.
- [9] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.
- [10] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.
- [11] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP Journ. on Wireless Commun. and Net.*, volume 2009, article ID 142374, 12 pages. doi:10.1155/2009/142374.
- [12] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.
- [13] N. R. Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71-74, Feb. 2012.
- [14] J. Xiong, K. K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496-1499, Sep. 2012.
- [15] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Tech.*, vol. 62, no. 5, pp. 2170-2181, Jun. 2013.
- [16] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536-2550, May 2013.
- [17] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge Univ. Press, 2004.
- [18] D. Guo, S. Shamai(Shitz), and S. Verdú, "Mutual information and minimum mean-square Error in Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1261-1282, Apr. 2005.
- [19] A. Lozano, A. M. Tulino, and S. Verdú, "Optimum power allocation for parallel Gaussian channels with arbitrary input distributions," *IEEE Trans. Inform. Theory*, vol. 52, no. 7, pp. 3033-3051, Jul. 2006.
- [20] J. Sturm, "Using SeDuMi 1.03: A MATLAB toolbox for optimization over symmetric cones," *Opt. Methods and Software*, vol. 11-12, pp. 625-653, 1999. Special issue on Interior Point Methods (CD supplement with software).
- [21] J. Lofberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," *Proc. CACSD Conf.*, Taipei, 2004. [Online] Available: <http://control.ee.ethz.ch/~joloef/yalmip.php>.